REMARKS/ARGUMENTS

The Applicant has amended claims to clarify that which the Applicant considers to be the invention. The Applicant respectfully submits that amendments to the claim set is fully supported by the originally filed specification.

Claim 7 has been amended to render claim 7 an independent claim to a system. Dependent claims 8-16 are unchanged and depend from independent system claim 7. Protocol method claims 1-6 are unchanged. It is respectfully submitted that this amendment addresses the objection under 37 CFR 1.75(c). Claim 7 has also been amended for clarity and imports certain features from original claim 1. Amended claim 7 is fully supported by reference to original claim 1 and original claim 7, and furthermore by reference to Fig. 4 and the associated description in the specification beginning at page 38.

In relation to the double patenting rejection a terminal disclaimer is filed in compliance with 37 CFR 1.321(c).

At pages 4-6 of the Office Action, the Examiner rejects claims 1, 3-5, 7-11 and 13-15 under 35 USC 102(e) as being anticipated by Shin *et al.* (US 5,987,134). A claim is only anticipated if all of its limitations are present in a single reference in the prior art. Because all the limitations of the claims of the present invention are not present in Shin *et al.*, as discussed below, the present invention is not anticipated by Shin *et al.* and the rejection is traversed. Reconsideration and withdrawal of the rejection is respectfully requested.

Shin *et al.* discloses a device for authenticating users access rights to resources. Shin *et al.* requires that access tickets are distributed to the users, whereby authentication of the users access rights to resources, such as execution control, can be performed. Shin *et al.* seeks to avoid the complexity occurring in the situation where both sides of user and protector use the same information for performing authentication (col. 3, lines 3-8).

Shin *et al.* discloses that the access ticket generation device 12 generates the access ticket 13 based on unique security characteristic information of the device 14 and the user identifying information 16, then the access ticket 13 is forwarded to the user (col. 5, lines 14-

18). The proving device 18 generates a response 19 by utilising the access ticket 13 and the user identifying information 16 and returns to the verification device 10 (col. 5, lines 21-23). The verification device 10 then verifies that the response has been generated based on the challenging data and the unique security characteristic information of the device (col. 5, lines 26-28).

This is a distinctly different system and means of achieving authentication than is claimed in the present application. Shin *et al.* relies on user identifying information, such as a password (col. 5, line 38) and a unique security characteristic of a device to authenticate a users access rights. This describes a very different invention to the presently claimed invention which does not seek to authenticate a users access rights, but instead, seeks to authenticate an untrusted chip.

It is respectfully submitted that there is little material overlap between Shin *et al.* and the presently claimed invention other than uncorrelated use of terms such as a verification device, a proving device, authentication, use of a random number and encryption/decryption techiques. Such features are separately well known, however, the present invention as defined in claim 1 recites a new and inventive validation protocol for authenticating a chip largely based on a process of comparing a decrypted random number with an original random number obtained from separate chips, being a trusted authentication chip (23 in Fig. 2) and an untrusted authentication chip (20 in Fig. 2). Validation is performed, in one embodiment, on system 21.

Shin *et al.* also discusses that the protection means may be hardware with a protecting effect (therein referred to as tamper-resistant hardware) against "theft of the inside conditions by external probes". A method of implementation of the tamper-resistant hardware is described (col. 5, lines 46-51). This further clearly differentiates Shin *et al.* from the present invention. It is this requirement that the present invention seeks to avoid. At page 4 of the present specification, under the heading "Authentication chips", the preferred embodiment of the present invention is described to avoid the problem of manufacturers resorting to specialised hardware or packaging and avoiding clone hardware. Shin *et al.* appears to rely on a physical protection means that is avoided by the validation protocol of the present invention.

The Examiner cites various disclosures from Shin *et al.* from col. 9, line 39 to col. 10, line 15 to demonstrate disclosure of various features of claim 1 (or currently amended claim 7) of the present application. However, further to the foregoing discussion, it is respectfully submitted that the random number generation means 102 discussed in Shin *et al.* is not the same as the use of random numbers as claimed in present claims 1 or 7. The Examiner is referred to Fig. 4 of the present specification as a preferred embodiment of the protocol of claim 1 and the system of claim 7. In the present invention, as claimed in claim 1, the random number R is generated and encrypted with an asymmetric encryption function E_{KT} using a first key (41). The trusted authentication chip 23 passes the encrypted random number R/E_{KT} to the untrusted authentication chip 20 after a call to the decryption process of chip 20 (see 42). Decryption of the encrypted random number with an asymmetric decryption function D using a secret key is performed at untrusted chip A (20) which returns a random number R (43) to system 21. System 21 compares R from 43 with the original random number R/E_{KT} from 41.

Nowhere is this process disclosed, taught or anticipated in the mentioned parts of Shin *et al.* Referring to Fig. 5 of Shin *et al.* response generation means 116 from proving device 11 and random number storing means 103 from verification device 10 interact at re-randomising means 123 on verification device 10. This is not a comparison of an original and a decrypted random number from separate chips as is claimed in claim 1 and independent claim 7 of the present application.

Similarly, nothing in Shin *et al.* teaches or suggests to one of ordinary skill in the art to modify the invention in Shin *et al.* to arrive at the presently claimed invention. Shin *et al.* is not directed at, and does not anticipate, a validation protocol for determining whether an untrusted authentication chip is valid by using an asymmetric encryption function to compare the random numbers obtained from separate chips.

For at least the aforementioned reasons, it is respectfully submitted that independent claims 1 and 7 of the present application are not anticipated by or obvious in light of Shin *et al*, likewise, the dependent claims of the present application are respectfully submitted to be patentable over Shin *et al.* when taken individually or in combination with any of the prior art of record.

CONCLUSION

In view of the foregoing, it is respectfully requested that the Examiner reconsider and withdraw the rejections under 35 USC 102(e) and 35 USC 103(a). The present application is believed to be in condition for allowance. Accordingly, the Applicant respectfully requests a Notice of Allowance of all the claims presently under examination.

Very respectfully,

Applicant:

SIMON ROBERT WALMSLEY

C/o: Silverbrook Research Pty Ltd
393 Darling Street
Balmain NSW 2041, Australia

Email: Kia.silverbrook@silverbrookresearch.com

Telephone: +612 9818 6633

Facsimile: +61 2 9818 6711